INNOVACIÓN TECNOLÓGICA EN ORGANIZACIONES CRIMINALES

Carmen Jordá Sanz*

Resumen

La innovación tecnológica criminal, más que un concepto, es un marco de análisis que parte de la comprensión de las organizaciones criminales como negocios lucrativos, de tal forma que se sirven de la evolución del mundo para adaptarse de la manera más efectiva y eficiente posible a él. En este contexto, la tecnología se postula como un medio de enorme capacidad innovadora para el crimen organizado en cuatro dimensiones: mediante su aprovechamiento directo para capacidades operativas, para la ampliación de mercados, para la optimización de sus ataques y para la manipulación de personas y colectivos de interés. Parece, por tanto, que las fórmulas de respuesta deberán contemplar estos postulados, y serán, por tanto, complejas y creativas si se desea adquirir un nivel de efectividad adecuado en esta lucha asimétrica y dinámica.

1. La innovación tecnológica criminal: concepto y funciones

En el contexto criminal, la consolidación y supervivencia de una organización depende, en gran medida, de su capacidad para adoptar estrategias empresariales eficaces; por tanto, como ocurre en el ámbito corporativo, el éxito en un negocio ilícito requiere la implementación de prácticas comerciales avanzadas. Sobre esta premisa, lo cierto es que las organizaciones criminales han demostrado una notable capacidad de adaptación al estudiar y replicar tácticas utilizadas por grandes corporaciones transnacionales. Desde la creación de una identidad de marca hasta la optimización del servicio al cliente, los líderes de los cárteles han adoptado estrategias empleadas por empresas como Walmart, McDonald's y Coca-Cola, lo que les ha permitido maximizar su alcance y rentabilidad en el mercado ilícito de drogas (Wainwright, 2018).

A modo de ejemplo, en torno a la creación de una identidad de marca el *narco-branding* se conoce como una estrategia de marca adoptada por los cárteles de droga con el objetivo de construir una identidad reconocible, proyectar poder, generar legitimidad y aumentar sus beneficios (Tamayo, 2023) y actualmente es notable su uso por parte del Cártel Jalisco Nueva Generación (CJNG) y el Cártel de Sinaloa mediante TikTok ofreciendo empleo a personas jóvenes y apoyo a madres solteras (Colegio de México, Northeastern Civic A.I. Lab, Seminario sobre Violencia y Paz, y Laboratorio de Odio y Concordia, 2024).

Particularmente la pandemia de la COVID-19 es un buen escenario ilustrativo sobre cómo las organizaciones criminales

* Profesora titular Universidad Camilo José Cela (UCJC), licenciada en Psicología y en Derecho, sexenio de investigación reconocido por la CNEAI (ANECA), Investigadora principal del grupo TECSEC a cargo del proyecto CRIMIDATA-UCJC. Mánager de Prosegur Research. cjorda@ucjc.edu

transnacionales demostraron una notable capacidad para optimizar su "servicio al cliente", adaptando sus operaciones a las nuevas condiciones sociales y económicas impuestas por la crisis. Esta adaptación se evidenció de diversas formas como muestra el interesante estudio de Anguita Olmedo y Miguel Gil (2021), que contiene numerosos ejemplos: el ofrecimiento de asistencia social en comunidades marginadas, cubriendo vacíos del Estado mediante la entrega de alimentos, productos sanitarios y medidas de control del orden público: en países como Brasil, El Salvador o México, grupos como Comando Vermelho, la Mara Salvatrucha y el Cártel de Sinaloa impusieron toques de queda, difundieron mensajes preventivos e incluso distribuyeron kits de higiene, presentándose como actores protectores en lugar de simplemente violentos; estas acciones no solo reforzaron su autoridad, sino que fortalecieron su relación con las comunidades, mejorando su imagen y generando fidelidad entre la población.

También, en el plano logístico, redes criminales vinculadas al narcotráfico ajustaron sus rutas y métodos de transporte para asegurar la continuidad del suministro de drogas, en especial hacia Europa. El uso intensivo del transporte marítimo, el almacenamiento previo de mercancía y el rediseño de métodos de ocultamiento permitieron mantener niveles récord de tráfico, como lo confirman las incautaciones registradas en puertos europeos durante los primeros meses de confinamiento. En paralelo, se detectó la inserción de estas redes en mercados emergentes de productos sanitarios, aprovechando la escasez y urgencia para vender mascarillas, test rápidos y medicamentos falsificados a través de plataformas digitales y redes sociales, muchas veces con sistemas de pago seguros y entregas rápidas, imitando el modelo de servicios de consumo formal.

Otro ámbito clave de esta optimización fue la digitalización de sus operaciones. El traslado masivo de actividades al entorno online permitió una reorganización operativa que incorporó elementos propios del comercio electrónico legal, atención al cliente a través de foros y estructuras de pago intermedio o *escrow*[1]. Estas prácticas, identificadas por Europol e Interpol durante la pandemia, reflejan una estrategia clara de gestión de riesgo y garantía de confianza para atraer y retener "clientes".

En conjunto, se entiende por tanto que la innovación criminal no solo consiste en desarrollar nuevas herramientas, sino en aplicar pensamiento creativo, flexibilidad y sentido de oportunidad a los medios requeridos para mantener y expandir mercados bajo presión. En un entorno global incierto, las redes criminales operan con una lógica empresarial que integra adaptación rápida, diversificación de servicios y sofisticación logística, consolidándose como actores económicos informales, pero altamente eficientes.

Entre las fórmulas de adaptación al mercado más relevantes destaca, lógicamente, la innovación tecnológica, que aplicada al entorno criminal se define como el uso y

[1] *Escrow* es una estructura de pago intermedio donde un tercero confiable retiene el dinero hasta que comprador y vendedor cumplen con lo acordado, garantizando seguridad para ambas partes.

adaptación de herramientas y avances tecnológicos de manera creativa y disruptiva para cometer delitos, cuyas ventajas incluyen la mejora en su eficiencia o de su eficacia, transformando el modus operandi tradicional de organizaciones o individuos involucrados en actividades ilícitas (Prosegur Research, 2022). Un ejemplo popular de innovación organizativa es la adopción de criptomonedas en mercados negros de la *dark web*[2] con el fin de realizar actividades de tráfico de drogas de forma más segura. De manera similar, tecnologías como los *deepfakes*[3], basadas en inteligencia artificial, han sido empleadas para extorsiones empresariales al manipular información visual y auditiva. Este entorno propicio para la manipulación de la información puede erosionar la confianza pública en las instituciones y, además, ser utilizado como herramienta para perpetrar fraudes, extorsiones y campañas de propaganda que legitimen o glorifiquen actividades delictivas a un nivel sin precedentes.

En este punto es conveniente recordar que la tecnología es un medio, que se puede disponer para fines lícitos o ilícitos, y que, como los ejemplos ilustran, las oportunidades que ofrecen las fórmulas de innovación consideradas para empresas son aplicables a todo tipo de organizaciones, incluyendo las criminales. El presente trabajo se va a limitar a realizar un análisis de las innovaciones tecnológicas conocidas en el crimen organizado, teniendo como propósito aportar elementos de análisis sobre el uso de innovaciones tecnológicas por parte de organizaciones criminales, especialmente en lo que respecta a la producción y tráfico de cocaína. A partir de información reciente y de casos documentados, se examinan algunas de las herramientas y prácticas tecnológicas que parecen haber contribuido a una mayor eficiencia en estas actividades ilícitas. El objetivo no es realizar una caracterización exhaustiva del fenómeno, sino contribuir a una mejor comprensión de ciertos mecanismos concretos de modernización dentro del crimen organizado.

El interés de este enfoque radica en que permite observar cómo las organizaciones criminales incorporan fórmulas de innovación tecnológica en su operativa, replicando esquemas propios de empresas legales. Para los responsables de políticas públicas, estos hallazgos pueden servir como insumo preliminar para el diseño de medidas que consideren los cambios tecnológicos dentro de la economía ilegal. Aun cuando las herramientas disponibles para combatir estas innovaciones siguen en desarrollo, contar con un conocimiento más detallado sobre cómo se estructura y transforma la oferta ilegal facilita la identificación de posibles puntos de intervención, tanto en términos preventivos como operativos. Asimismo, esta línea de investigación puede complementarse con estudios posteriores que amplíen el análisis hacia otros productos y servicios ilegales

[2] La *dark web* es una sección no indexada de Internet que se encuentra deliberadamente oculta y a la que solo se puede acceder mediante software especializado; en este entorno se facilita el anonimato de los usuarios, permitiendo tanto actividades legítimas como ilícitas.

[3] Los *deepfakes* constituyen una técnica avanzada de manipulación digital que emplea inteligencia artificial para generar contenidos audiovisuales falsificados, en los que se recrean rostros, expresiones faciales y voces humanas de manera hiperrealista. Esta tecnología plantea serias implicaciones en materia de desinformación, suplantación de identidad y vulneración de la integridad informativa.

o entornos digitales utilizados por estas redes.

En el presente análisis, el concepto de innovación tecnológica criminal incluye la adopción de nuevas tecnologías en procesos y estrategias delictivas, las cuales pueden analizarse bajo diversos modelos teóricos vinculados a las oportunidades tecnológicas desde una doble perspectiva criminal y empresarial. Así, el modelo de la Triple Hélice, planteado por Etzkowitz y Leydesdorff (1995), resalta la colaboración entre universidades, empresas y gobiernos para fomentar la innovación; sin embargo, en el ámbito criminal, esta dinámica se replica constantemente mediante alianzas, por ejemplo, entre hackers y empleados bancarios corruptos, como en los ataques al sistema SWIFT[4]. También con colaboraciones entre expertos en biotecnología y redes ilícitas para desarrollar drogas sintéticas indetectables, mostrando cómo el crimen organizado explota la innovación científica. Así, la producción mundial de cocaína ha aumentado significativamente debido a mejoras tecnológicas en la extracción del alcaloide y a la optimización de los cultivos. Esto ha resultado en una mayor productividad por hectárea cultivada, ya que nuevas variedades de coca —de mayor concentración alcaloide— han sido adoptadas de forma sistemática, especialmente en Colombia. Este país, de hecho, registró en 2023 un récord histórico con 230.000 hectáreas sembradas y un aumento del 24 % en la producción potencial de cocaína, alcanzando las 1.738 toneladas métricas, lo que representa un incremento del 53 % respecto al año anterior (UNODC, 2024a). Este salto productivo no se debe a una expansión territorial descontrolada, sino a una mayor eficiencia en la transformación de materia prima.

Estos datos reflejan cómo las organizaciones criminales han adoptado un enfoque técnico-científico en la producción de cocaína, aplicando mejoras en sus procesos y expandiendo sus operaciones con criterios empresariales. La innovación en este contexto no es improvisada, sino estratégica: implica flexibilidad, adaptabilidad y pensamiento creativo orientado a maximizar la eficiencia y mantener la resiliencia operativa frente a las presiones del Estado y el mercado.

La innovación tecnológica criminal ha permitido que las organizaciones ilícitas aprovechen de manera más efectiva las denominadas zonas grises, lo que implica un cambio significativo en la concepción tradicional de la seguridad. Según Jordán (2018), tanto las grandes potencias como los actores no estatales emplean estrategias ambiguas y graduales para maximizar sus intereses sin provocar conflictos abiertos. Este enfoque también es adoptado por organizaciones criminales, que se benefician de la ambigüedad normativa y la falta de respuestas contundentes, optimizando sus operaciones mediante tecnologías avanzadas como drones, ciberataques y sistemas de vigilancia. A través de modelos de negocio sofisticados, estas entidades operan en espacios poco controlados, maximizando sus beneficios mientras minimizan los riesgos de intervención estatal. La tecnología juega un papel cla-

[4] El sistema SWIFT (Society for Worldwide Interbank Financial Telecommunication) constituye una infraestructura de mensajería electrónica estandarizada que posibilita la comunicación segura entre entidades financieras a escala global.

ve en este proceso, permitiendo que grupos criminales se coordinen y actúen de manera eficiente y beneficiosa.

La innovación tecnológica también afecta a la seguridad y defensa, tal como señala Abad Soto (2025), quien argumenta que el uso de tecnologías avanzadas en el ámbito militar, como drones y robots autónomos, está acelerando las operaciones y ofreciendo nuevas oportunidades a actores ilícitos. De manera similar, la integración de herramientas como la impresión 3D y los vehículos no tripulados facilita la fabricación y transporte de materiales ilegales, mientras que la creciente conectividad y el uso de *nubes de combate*[5] optimizan las capacidades de inteligencia y mando de estos grupos. En conjunto, la convergencia entre la lógica de la zona gris y la innovación tecnológica criminal aumenta la complejidad de las respuestas estatales, ya que las operaciones ilícitas se desarrollan en un umbral de conflicto difuso y difícil de detectar (Jordán, 2018; Abad Soto, 2025).

2. La innovación tecnológica por parte de la delincuencia organizada

La innovación tecnológica criminal, como se ha señalado previamente, es un concepto amplio y complejo; para acotar el objeto de estudio se identifican cuatro dimensiones fundamentales desde las cuales es posible analizar las principales innovaciones criminales actualmente reconocidas: (1) el aprovechamiento de los avances tecnológicos; (2) la potenciación de los mercados del crimen organizado; (3) la optimización de los ataques; y, finalmente, (4) el hackeo de la mente (Prosegur Research, 2022).

El aprovechamiento de los avances tecnológicos ha permitido a las organizaciones criminales maximizar sus capacidades operativas, reduciendo tanto los costos como los riesgos asociados a sus actividades ilícitas. Un caso notorio fue cuando en 2021 la Policía Nacional desmanteló el primer taller ilegal de impresión de armas 3D detectado en España —y en Alemania en 2019— mediante el que se advirtió su potencial despliegue para usos terroristas y criminales. En el sudeste asiático, redes criminales han incorporado inteligencia artificial generativa y tecnología de *deepfakes* en estafas conocidas como *pig butchering*[6]; estas técnicas permiten crear identidades falsas convincentes y contenido personalizado en múltiples idiomas, facilitando la manipulación de víctimas en esquemas de inversión fraudulentos (Burgess y Newman, 2024). Además, se utilizan herramientas como *crypto drainers*[7] para vaciar carteras de criptomonedas de las víctimas. La UNODC (2024b)

[5] Las nubes de combate son infraestructuras tecnológicas avanzadas desarrolladas para entornos militares, basadas en la computación en la nube y la inteligencia artificial, que permiten la integración en tiempo real de sensores, plataformas y sistemas de mando y control, optimizando la recopilación, análisis y distribución de datos estratégicos para la toma de decisiones operacionales.

[6] *Pig butchering* es una modalidad de estafa cibernética en la que los delincuentes ganan la confianza de las víctimas —a menudo mediante redes sociales o aplicaciones de citas— para manipularlas emocionalmente y convencerlas de invertir grandes sumas en esquemas fraudulentos con criptomonedas.

[7] *Crypto drainers* hace referencia a programas maliciosos que permiten a los atacantes vaciar automáticamente las billeteras de criptomonedas de las víctimas una vez que estas interactúan con enlaces o contratos inteligentes manipulados, facilitando el robo masivo de activos digitales.

estima que estas operaciones generaron ingresos de hasta 37 mil millones de dólares en 2023.

La potenciación de los mercados del crimen organizado mediante el uso de tecnologías avanzadas ha dado lugar a un fenómeno global, que incluye el auge de los criptomercados y el perfeccionamiento de los métodos de producción y transporte de sustancias ilícitas y de blanqueo de capitales. Los criptomercados, operando a través de redes descentralizadas como la *darkweb*, permiten a las organizaciones que así lo busquen, operar en el ciberespacio en sus actividades de intercambio de bienes y servicios ilegales, como drogas, armas o información confidencial, utilizando plataformas que dificultan la trazabilidad de las transacciones (Jordá, Píriz y Gimenez-Salinas, 2024).

Otro ejemplo se identifica al analizar como las organizaciones criminales han explotado plataformas de juegos de azar online y proveedores de activos virtuales no regulados para blanquear grandes sumas de dinero (UNODC, 2024b); además de ampliar mercados estas plataformas permiten mover y blanquear fondos ilícitos con mayor facilidad, aprovechando la falta de supervisión en ciertas jurisdicciones. Además, el uso de narcosubmarinos, barcos y otros métodos de transporte sofisticados para el traslado de drogas (Insight Crime, 2024) como el caso informado por la Royal Navy sobre la interceptación de un narcosubmarino en el Mar Caribe, resultando en la incautación de 2.000 kg de cocaína con un valor estimado de £160 millones. Un caso aún más emblemático fue el submarino que cruzó el Amazonas y el Atlántico desde Colombia hasta Galicia (*Infobae*, 2021) evidenciando la capacidad logística y tecnológica, así como financiera para construir o adquirir y desechar rápidamente tras su uso de rápida amortización dado el alto nivel lucrativo de sus actividades. Estas innovaciones, a su vez, aportan un alto valor en términos de impunidad en los espacios marítimos, de alta rentabilidad y menor riesgo.

La optimización de los ataques a través de tecnologías avanzadas ha permitido a las organizaciones criminales ejecutar operaciones con mayor precisión, alcance y sofisticación, de forma paralela a lo ocurrido en grupos terroristas. Uno de los ejemplos más notables en este ámbito es el uso de drones: estos dispositivos han evolucionado desde su empleo inicial para el transporte de drogas y materiales entre fronteras, o incluso dentro de las prisiones, hasta su adopción en ataques directos. En los últimos años, las organizaciones criminales en América Latina han incorporado drones como herramientas estratégicas, ampliando su uso desde el transporte de drogas y objetos ilícitos hasta la ejecución de ataques directos con explosivos contra fuerzas del orden, poblaciones rivales y objetivos estratégicos. Esta evolución tecnológica refleja un preocupante proceso de militarización de los recursos delictivos, así como una creciente capacidad de innovación táctica por parte de grupos armados ilegales.

El CJNG ha incorporado drones modificados para lanzar explosivos en sus operaciones, especialmente en Michoacán. Se han documentado ataques contra fuerzas de seguridad y poblaciones rivales. Por ejemplo, en Cotija, Michoacán, un ataque

con drones resultó en la muerte de un militar y varios heridos. Además, se ha identificado una unidad especializada dentro del cártel, conocida como "Operadores Droneros", encargada de estas operaciones (*Infobae*, 2023; *El Universal*, 2023).

Los drones se utilizan no solo para el transporte de explosivos hacia sus objetivos, sino también para ataques a autoridades policiales u organizaciones competidoras, en lo que se ha denominado "guerra tecnológica". En el contexto del CJNG y los Cárteles Unidos, por ejemplo, los drones han sido utilizados para ejecutar ataques contra rivales, evidenciando la creciente integración de tecnologías avanzadas en los conflictos del crimen organizado (Mayen, 2025). También ha habido un incremento significativo en el uso de drones por parte de organizaciones criminales para el transporte de drogas y la vigilancia de las fuerzas de seguridad en la frontera entre México y Estados Unidos (JIFE, 2025); estos dispositivos permiten a los cárteles monitorear los movimientos de las autoridades y facilitar el cruce de estupefacientes, representando un desafío creciente para las estrategias de seguridad fronteriza

El hackeo de la mente se refiere a las técnicas utilizadas para manipular la percepción y conducta de los individuos mediante el uso de tecnologías de la información. Entre las principales técnicas empleadas por las organizaciones criminales se incluyen el *phishing*[8], el *vishing*[9] —o suplantación telefónica—, y el uso de *deepfakes*. El *phishing* y el *vishing* buscan engañar a las personas para que proporcionen información sensible, como contraseñas o detalles financieros, como el caso de la red criminal internacional que obtenía credenciales de usuarios para desbloquear dispositivos móviles robados y acceder a información personal sensible; la organización operaba desde hacía al menos cinco años, afectando a más de 483.000 víctimas en países como España, Argentina, Colombia, Chile, Ecuador y Perú, administrando la plataforma iServer, utilizada para generar páginas web fraudulentas que simulaban ser oficiales de fabricantes de teléfonos, engañando a las víctimas para que proporcionaran sus datos de acceso (Viúdez y Lorca, 2024). En cambio, los *deepfakes* permiten la creación de videos falsificados que pueden ser utilizados para difamar, manipular o engañar a una audiencia, como por ejemplo para estafar simulando ser un personaje conocido (Peralta, 2024). Se destaca el caso de La Tropa del Infierno, brazo armado del Cártel del Noreste, que entrena y emplea a niños sicarios (Tapia Sandoval, 2025).

Particularmente, las organizaciones criminales utilizan la desinformación desde información transmitida por sus medios

[8] El *phishing* es una modalidad de ataque informático basada en técnicas de ingeniería social, mediante la cual los atacantes suplantan la identidad de entidades legítimas a través de correos electrónicos, mensajes o sitios web fraudulentos, con el fin de obtener información confidencial del usuario, como credenciales de acceso o datos financieros.

[9] El *vishing*, abreviatura de *voice phishing*, es una variante del *phishing* que se realiza mediante llamadas telefónicas; en este tipo de ataque, los ciberdelincuentes utilizan técnicas de manipulación verbal, a menudo mediante grabaciones automatizadas o falsas representaciones institucionales, para inducir a la víctima a revelar datos personales o financieros.

para moldear la percepción pública a su favor, al generar narrativas falsas o confusas, las organizaciones criminales logran operar con mayor impunidad y evadir la detección. Por ejemplo, en el caso de Los Pulpos, una banda criminal que opera en Perú y Chile, han utilizado tácticas de desinformación para encubrir sus actividades y manipular la percepción pública sobre sus operaciones (Gómez Vega, 2025).

3. Tendencias en la innovación tecnológica criminal

En este punto, más que tendencias criminales específicas, conviene entender el entorno de las tendencias tecnológicas de las que el crimen organizado, en tanto que negocio, se sirve en su evolución y adaptación al mundo. Así, la innovación criminal del futuro estará marcada por la velocidad de adopción y adaptación de nuevas tecnologías, un fenómeno acelerado por el crecimiento exponencial de las tecnologías emergentes y la inversión en avances como la inteligencia artificial, el internet de las cosas (IoT) y la computación en la nube (Rojas, 2016; Morelos-Gómez *et al*., 2023). Estos desarrollos han evolucionado rápidamente en los últimos años, y la preocupación por su regulación efectiva y segura es ahora una prioridad de Estado para muchos gobiernos y empresas. Lógicamente, estas mismas innovaciones presentan oportunidades significativas para actores criminales de diversa índole, quienes buscan explotar las carencias y vacíos de las normativas de seguridad digital y la infraestructura global (Sánchez, 2021; Moreno Jorge *et al*., 2023).

Así, las grandes tendencias delineadas por el Gobierno británico sobre las claves tecnológicas en seguridad tienen implicaciones fundamentales (Home Office, 2019). En primer lugar, el crecimiento exponencial acelerado de datos y tecnologías permite a los grupos criminales aprovechar una cantidad significativamente mayor de información, lo que incrementa su capacidad para diseñar y ejecutar actividades ilícitas con mayor precisión y eficacia. Así, las organizaciones han incorporado inteligencia artificial, análisis automatizado de grandes volúmenes de datos y algoritmos de aprendizaje automático para personalizar ataques, seleccionar víctimas con mayor eficacia y ejecutar fraudes a escala industrial: a través de técnicas como la generación de identidades falsas, el uso de *deepfakes*, la clonación de voces y el despliegue de *chatbots* multilingües, el crimen organizado logra diversificar sus operaciones con niveles crecientes de sofisticación tecnológica. Además, se valen de plataformas de mensajería encriptada y foros clandestinos para comercializar desde *malware* hasta datos financieros robados; de este modo, expanden su alcance operativo mientras reducen la necesidad de contacto directo. Tecnologías como el *Malware-as-a-Service*[10] o servicios como *clouds of logs*[11] permiten que incluso actores sin

[10] *Malware-as-a-Service* (MaaS) es un modelo delictivo en el que cibercriminales alquilan o venden *malware* listo para usar a otros usuarios a través de plataformas en línea, facilitando ataques sin necesidad de conocimientos técnicos avanzados.

[11] *Clouds of logs* son servicios que almacenan y venden grandes volúmenes de registros digitales (logs), como historiales de navegación, credenciales o actividad en sistemas comprometidos, utilizados frecuentemente para fraudes o ciberespionaje.

conocimientos técnicos puedan participar en esquemas criminales avanzados; en conjunto, estas herramientas reducen las barreras de entrada al delito digital, transformando las estructuras criminales en ecosistemas dinámicos y altamente adaptables (UNODC, 2024b).

Este fenómeno está íntimamente relacionado con la convergencia tecnológica, que no solo potencia la complejidad de las actividades criminales, sino que también les permite integrar herramientas que antes eran inconcebibles para su accionar, facilitando la creación de infraestructuras ilegales virtuales más sofisticadas. La integración simultánea de múltiples herramientas digitales que permiten crear entornos virtuales criminales cada vez más complejos y eficientes: ejemplos de ello son los mercados ilegales en Telegram donde los grupos criminales combinan funciones bancarias, intercambio de criptomonedas, servicios de garantía, logística de fraude y venta de software malicioso en un solo ecosistema; estas plataformas operan como verdaderas infraestructuras paralelas del delito, sin anclaje territorial ni regulación estatal efectiva (UNODC, 2024b).

La automatización de procesos y roles, por su parte, tiene un impacto directo en la capacidad operativa de los actores criminales, permitiéndoles reducir costos, incrementar la escala de sus operaciones y ejecutar actividades ilícitas con una precisión y eficiencia sin precedentes. Esto se complementa con la difusión de la frontera entre lo *online* y *offline*, lo cual permite al crimen organizado operar en un entorno cada vez más hibrido, donde lo físico y lo digital se interrelacionan de formas complejas. La integración de plataformas cibernéticas y redes sociales en el ejercicio del crimen permite a los actores no solo ejecutar ataques virtuales, sino también coordinar actividades en el mundo físico, como la distribución de drogas o el secuestro de personas. En este contexto, la adopción de contratos inteligentes y el uso de *crypto drainers* permite automatizar el vaciado de carteras digitales de las víctimas sin necesidad de intervención humana directa; este tipo de herramientas, típicas de la innovación financiera legítima, han sido reapropiadas con fines criminales, ampliando la autonomía operativa de estas redes delictivas (UNODC, 2024b).

Finalmente, el empoderamiento de actores diversos, incluidos criminales, ha dado lugar a una democratización del acceso a herramientas de cibercrimen, lo que permite que grupos más pequeños o menos estructurados adopten tecnologías avanzadas para llevar a cabo delitos de forma eficiente. Esto implica que, aunque las innovaciones tecnológicas abren nuevas posibilidades para el crimen organizado, también plantean desafíos en términos de control y regulación por parte de los actores estatales. No obstante, como se observa en el ámbito empresarial, la innovación tecnológica no garantiza el éxito si no se adapta a un ecosistema colaborativo que considere las necesidades y dinámicas de las partes involucradas. De manera similar, el crimen organizado también debe ajustar sus métodos a las nuevas realidades digitales, lo que lo obliga a adaptarse continuamente a un entorno volátil y cambiante.

A modo de ejemplo, EncroChat fue una red de comunicación cifrada utilizada ampliamente por organizaciones criminales para coordinar actividades ilícitas de forma aparentemente segura, que ofrecía teléfonos personalizados con funciones limitadas y un sistema de mensajería encriptada de extremo a extremo. Las operaciones Venetic en el Reino Unido y Emma 95 en Francia, que culminaron en 2020 con el apoyo de Europol y Eurojust, lograron infiltrarla y descifrar millones de mensajes, revelando una vasta red de tráfico de drogas, armas y blanqueo de capitales, entre otros delitos. Este caso evidenció cómo el crimen organizado invierte en infraestructura tecnológica propia, pero también cómo la cooperación internacional y el trabajo forense digital pueden contrarrestar incluso sistemas altamente protegidos. Y un paso más allá: llama la atención la escasez de operaciones exitosas contra redes de comunicación cifrada como EncroChat, especialmente si se considera su uso extendido en el crimen organizado. A pesar de que estas plataformas se han convertido en infraestructuras clave para la coordinación de actividades ilícitas a gran escala, las intervenciones estatales han sido limitadas y excepcionalmente complejas desde el punto de vista técnico y legal. Las fórmulas de detección y cierre deben ser estudiadas para que no su éxito no sea una excepción.

En este punto del análisis es pertinente destacar el concepto de *Crime as a Service* (CaaS), un término introducido por Europol en 2014 para describir un modelo de negocio en el ámbito virtual donde se ofrecen diversos servicios delictivos mediante la venta o alquiler de herramientas, infraestructura y conocimientos especializados relacionados con actividades ilegales en línea; es precisamente en este entorno, la innovación tecnológica criminal se vuelve más accesible y rentable. Un ejemplo representativo de los servicios ofrecidos en el modelo de *Crime as a Service* (CaaS) es la comercialización de kits de *phishing* automatizados, los cuales incluyen plantillas de páginas web falsas, servidores de alojamiento, herramientas para el robo de credenciales y paneles de administración para la gestión de víctimas, que se venden o alquilan en foros clandestinos y mercados de la Dark Web, facilitando que actores con escaso conocimiento técnico puedan ejecutar campañas fraudulentas de manera eficaz.

Este tipo de servicios delictivos mediante la venta o alquiler de herramientas, infraestructura y conocimientos especializados relacionados con actividades ilegales en línea ilustra cómo la innovación tecnológica ha sido apropiada por redes criminales. Es precisamente en este entorno donde la *innovación tecnológica criminal* se vuelve un factor multiplicador de capacidades, favoreciendo la descentralización, profesionalización y escalabilidad de las operaciones ilícitas. El modelo CaaS permite así reducir barreras de entrada para nuevos actores y amplía significativamente el alcance del cibercrimen global a manos de organizaciones no necesariamente especializadas en estos ámbitos.

4. Conclusiones: contra la innovación, más innovación

Las organizaciones criminales, al igual que cualquier otra organización que opere en el mundo legal, deben ser entendidas como corporaciones en todos los aspectos

clave de su funcionamiento, incluyendo sus fórmulas de productividad y lucro. Al analizar el crimen organizado a través de esta perspectiva, podemos identificar que, como estructuras empresariales buscan, ante todo, maximizar sus beneficios mediante la explotación de recursos, el empleo de mano de obra y la implementación de estrategias de innovación. Sin embargo, la diferencia radica en que los métodos y objetivos de estas organizaciones suelen tener un carácter ilícito, lo que plantea un reto adicional para su comprensión y erradicación. Por ello, es imprescindible estudiarlas como organizaciones en toda su complejidad, analizando no solo sus métodos tradicionales de generación de beneficios, sino también la forma en que incorporan la innovación tecnológica a sus estrategias operativas.

La absorción y apropiación ilícita de innovaciones tecnológicas y tendencias emergentes del ámbito legal es un fenómeno que no debe sorprender, ya que estos avances ofrecen herramientas que pueden ser explotadas para fines delictivos. Sin embargo, ello no debe limitar, en modo alguno, el desarrollo de empresas prósperas, administraciones públicas eficientes y, sobre todo, una ciudadanía avanzada y civilizada, que haga uso responsable de la tecnología disponible.

Para contrarrestar y comprender estos desafíos, resulta fundamental que las organizaciones dedicadas a la lucha contra el crimen organizado adopten una perspectiva amplia e integral, que incluya la colaboración activa con el ámbito académico. La ciencia, si bien no siempre es la metodología más eficiente en términos de resultados inmediatos, se postula como el método más efectivo para desentrañar la complejidad inherente a estos fenómenos. En este sentido, la integración de las ciencias de la informática, las ciencias físicas y las ciencias sociales constituye un pilar fundamental para comprender y enfrentar los desafíos relacionados con la seguridad y la inseguridad en el contexto actual. En primer término, las tecnologías de la información y las comunicaciones (TIC), la criptografía y la digitalización de las empresas, junto con el diseño de entornos híbridos (phygital), ofrecen herramientas esenciales para mejorar la seguridad. Estas tecnologías permiten, por un lado, optimizar la protección de infraestructuras críticas y, por otro, evidencian vulnerabilidades que pueden ser aprovechadas para actividades delictivas, como el tráfico ilegal y los delitos contra el patrimonio.

Por otro lado, las ciencias físicas —abarcando disciplinas como la física, la química, la biología, la nanotecnología y las tecnologías nucleares y cuánticas— son cruciales para comprender y mitigar las amenazas que surgen de la convergencia tecnológica. El análisis de estos avances posibilita la detección de nuevas formas de guerra tecnológica, el desarrollo de sistemas autónomos y la implementación de métodos avanzados de control e identificación, que pueden ser empleados tanto en contextos legítimos como ilícitos.

Finalmente, las ciencias sociales, a través de la criminología, la psicología y la sociología, aportan un marco interpretativo indispensable para entender la conducta antisocial y delictiva. El estudio de los procesos de cambio demográfico, la construcción de la identidad social y la evaluación de las dinámicas comunitarias

facilitan la formulación de políticas públicas y marcos jurídicos adecuados para prevenir y sancionar conductas delictivas. Este enfoque resulta vital para interpretar los fenómenos delictivos en un contexto de constante transformación social.

Así, para hacer frente a la creciente innovación criminal, los Estados deben adoptar una estrategia integral que combine prevención, regulación tecnológica, disuasión penal y cooperación internacional. A nivel individual, los gobiernos pueden comenzar por fortalecer sus capacidades técnicas, invirtiendo en inteligencia artificial, análisis de datos y ciberseguridad, con el fin de detectar patrones delictivos emergentes y anticiparse a nuevas formas de criminalidad.

En paralelo, deben promover marcos regulatorios más ágiles y especializados, capaces de adaptarse a tecnologías que pueden ser utilizadas tanto para fines legítimos como para actividades delictivas. Esto implica también colaborar activamente con el sector privado y la academia para fomentar una gobernanza tecnológica responsable.

La cooperación internacional, por su parte, resulta esencial, especialmente en ámbitos como el cibercrimen, el tráfico de drogas o el crimen organizado transnacional, donde las fronteras legales se desdibujan. Compartir inteligencia, armonizar normativas, fortalecer redes como Europol, INTERPOL o UNODC, los facilitadores y potenciadores de las operaciones conjuntas marcarán la continuidad y mejora de las mismas, debiendo considerarse vías efectivas para contener la expansión de capacidades criminales.

Además, es clave aumentar los costes de innovar para las organizaciones criminales. Esto se logra dificultando el acceso a tecnologías críticas, atacando las infraestructuras logísticas mediante acciones específicas (como el cierre de laboratorios, interceptación de cargamentos o desmantelamiento de redes de soporte técnico), poniendo el foco en las fuentes de financiación e innovación para frenar su crecimiento como organización.

Finalmente, las ciencias sociales también deben jugar un rol operativo, generando evidencia para diseñar políticas de prevención centradas en contextos sociales de riesgo, reduciendo así la base de reclutamiento y la tolerancia social hacia estos grupos.

En definitiva, en un escenario de fuerzas asimétricas donde el crimen organizado se desenvuelve sin reparos ante situaciones poco éticas o directamente ilegales, solo la capacidad intelectual en favor de la innovación puede dotarnos de una defensa efectiva. Por ello, la respuesta innovadora frente a las estrategias delictivas debe estar marcada por soluciones nunca antes dadas, capaces de contrarrestar de manera eficaz el dinamismo del fenómeno criminal. Es imperativo que la ciencia y la creatividad sean los pilares que orienten el desarrollo de estrategias y herramientas, adoptando un enfoque que combine la audacia necesaria para combatir el delito con el respeto hacia los derechos y las libertades civiles, buscando la eficiencia de las medidas implementadas con todos los recursos, incluyendo los tecnológicos, a su alcance.

Esta aproximación multidisciplinar y valiente, que integre conocimientos y técnicas de diversos campos, permitirá la formulación de respuestas de largo alcance, adaptadas a la complejidad y dinamismo del entorno actual. Así, el enfrentamiento contra el crimen organizado se convierte en un proceso continuo de aprendizaje y adaptación, en el que la innovación contra la innovación se erige como el camino más prometedor para asegurar la protección de la sociedad frente a amenazas en constante evolución.

5. Resumen de ideas finales

La innovación tecnológica criminal, más que un concepto, se concibe como un marco de análisis en el que estudiar el crimen organizado desde la comprensión de su faceta empresarial, adaptándose de forma continua a los cambios tecnológicos y sociales para maximizar la eficiencia y efectividad en sus operaciones ilícitas, aprovechando la evolución tecnológica para innovar sus métodos.

Según el presente análisis, se identifican cuatro dimensiones sobre las que las organizaciones criminales innovan tecnológicamente. Para dificultar la mejora operativa de las organizaciones criminales, los Estados pueden invertir en capacidades tecnológicas propias, que permitan anticipar patrones y detectar infraestructuras críticas delictivas. En cuanto a su expansión de mercados, la cooperación internacional y la armonización normativa resultan clave para cerrar vacíos legales y bloquear rutas transnacionales. Para frenar la optimización de ataques, es necesario regular tecnologías de uso dual (como drones o cifrado), además de desarrollar sistemas de defensa adaptativa y contrainteligencia digital con un asesoramiento técnico de expertos. Finalmente, frente a la manipulación de colectivos, el fortalecimiento de la alfabetización mediática, la regulación de contenidos en plataformas digitales y la intervención estratégica en entornos vulnerables son fundamentales para reducir la influencia social de los grupos criminales.

Para enfrentar estos desafíos, es fundamental adoptar una perspectiva integral que involucre la colaboración académica, sin limitar el desarrollo de las empresas y los derechos y libertades de la ciudadanía. La integración de las ciencias de la información, ciencias físicas y ciencias sociales resulta clave para comprender el fenómeno y diseñar estrategias de seguridad de forma anticipada y preventiva.

Ante un entorno asimétrico en el que el crimen organizado no conoce límites legales ni éticos, solo la capacidad intelectual en favor de la innovación ofrece una defensa eficaz. Así, la lucha contra el crimen organizado se convierte en un proceso continuo de aprendizaje y adaptación, donde la innovación contra la innovación criminal es la estrategia más prometedora para proteger a la sociedad frente a amenazas en constante evolución.

Referencias bibliográficas

ANGUITA OLMEDO, C. Y MIGUEL GIL, J. (2021): "El crimen organizado transnacional en la era digital: (Re)adaptación a la crisis de la COVID-19", en FIGUEREO-BENÍTEZ, J. C. y MANCINAS-CHÁVEZ, R. (eds.), *Las redes de la comunicación. Estudios multidisciplinares actuales,* Dykinson, pp. 38-60. Disponible en: https://idus.us.es/items/5a0cbd05-97ef-4825-957e-1251023b40b1.

ABAD SOTO, J. (2025): *Cambio de paradigma de la seguridad y la defensa: capacidades futuras, ya presentes*, Documento de Opinión IEEE 04/2025. Disponible en: https://www.defensa.gob.es/ceseden/-/ieee/cambio_de_paradigma_de_la_seguridad_y_la_defensa_2025_dieeeo04.

EL COLEGIO DE MÉXICO, Northeastern Civic A.I. Lab, Seminario sobre Violencia y Paz, y Laboratorio de Odio y Concordia (2024): *Nuevas fronteras en el reclutamiento digital: Estrategias de reclutamiento del crimen organizado en TikTok*. Disponible en: https://violenciaypaz.colmex.mx/publicacion/nuevas-fronteras-en-el-reclutamiento-digital-estrategias-de-reclutamiento-del-crimen-organizado-en-tiktok.

BURGESS, M. Y NEWMAN, L. H. (2024): "Pig butchering scams are going high tech", *Wired*, 12 de octubre. Disponible en: https://www.wired.com/story/pig-butchering-scams-go-high-tech/?.

EL UNIVERSAL (2023): "CJNG ataca con drones explosivos al Ejército en Cotija, Michoacán; hay seis militares lesionados y uno más muerto", 10 de febrero. Disponible en: https://www.eluniversal.com.mx/estados/cjng-ataca-con-drones-explosivos-a-ejercito-mexicano-en-cotija-michoacan-hay-seis-militares-lesionados-y-uno-mas-muerto/.

EUROPEAN UNION AGENCY FOR CYBERSECURITY, ENISA (2024): *ENISA threat landscape 2024*. Disponible en: https://rb.gy/3otdrw.

EUROPOL (2013): *Serious and Organised Crime Threat Assessment (SOCTA) 2013*, Publications Office of the European Union. Disponible en: https://www.europol.europa.eu/publications-events/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013.

— (2021): *European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021: A corrupting influence – The infiltration and undermining of Europe's economy and society by organised crime*, Publications Office of the European Union. Disponible en: https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021.

— (2025): *European Union Serious and Organised Crime Threat Assessment (SOCTA) 2025*, Publications Office of the European Union. Disponible en: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

ETZKOWITZ, H. Y LEYDESDORFF, L. (1995): "The triple helix: University-industry-government relations: A laboratory for know-ledge-based economic development", *EASST Review*.

GÓMEZ VEGA, R. (2025): "Los Pulpos, la banda de cuatro hermanos que siembra el terror en Perú y Chile", *El País*, 22 de febrero. Disponible en: https://elpais.com/chile/2025-02-22/los-pulpos-la-banda-de-cuatro-hermanos-que-siembra-el-terror-en-peru-y-chile.html.

HOME OFFICE (2019): *Future technology trends in security*. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786244/HO_OSCT_Future_Tech_Trends_Final_Updated_13Mar19.pdf

JUNTA INTERNACIONAL DE FISCALIZACIÓN DE ESTUPEFACIENTES, JIFE (2025): *Informe anual 2024*, Organización de las Naciones Unidas. Disponible en: https://www.incb.org/documents/Publications/AnnualReports/AR2024/Annual_Report/E-INCB-2024-1-ENG.pdf.

JORDÁ, C., PÍRIZ, C. Y GIMÉNEZ-SALINAS, A. (2024): "Los criptomercados ilícitos de tráfico de drogas en la Dark Web: Un estudio exploratorio empírico", *Revista Española de Investigación Criminológica, 22*(2), e884. Disponible en: https://reic.criminologia.net/index.php/journal/article/view/884/415.

JORDÁN, J. (2018): "El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo", *Revista Española de Ciencia Política*, 48, pp. 129-151.

INFOBAE (2021): "La increíble historia del narcosubmarino que cruzó el Atlántico y fracasó en su misión sobre el final", 16 de octubre. Disponible en: https://www.infobae.com/def/2021/10/16/la-increible-historia-del-narcosubmarino-que-cruzo-el-atlantico-y-fracaso-en-su-mision-sobre-el-final/.

— (2023): "Quiénes son los 'Operadores droneros', la unidad del CJNG especializada en ataques con explosivos", 1 de junio. Disponible en: https://www.infobae.com/mexico/2023/06/01/quienes-son-los-operadores-droneros-la-unidad-del-cjng-especializada-en-ataques-con-explosivos/.

INSIGHT CRIME (2024): "Narcosubmarinos navegan por el Caribe", 19 de septiembre. Disponible en: https://insightcrime.org/es/noticias

/traficantes-caribenos-narcosubmarinos-eludir-operaciones-antinarcoticos/.

MAYEN, B. (2025): "Difunden video de un ataque con drones en Río Bravo, Tamaulipas: 'Se murieron todos'", *Infobae*, 3 de febrero. Disponible en: https://www.infobae.com/mexico/2025/02/03/difunden-video-de-un-ataque-con-drones-en-rio-bravo-tamaulipas-se-murieron-todos/.

MORELOS-GÓMEZ, J., TIRADO-ROCA, S. Y GUERRERO ÁLVAREZ, L. M. (2023): "Innovación en las organizaciones: Una revisión de la literatura", *Dictamen Libre*. Disponible en: https://revistas.unilibre.edu.co/index.php/dictamenlibre/article/download/10404/9779.

MORENO JORGE, M., PORRAS ARAGON, J. I. Y CÉSPEDES GONZALES, C. M. (2023): Uso de herramientas tecnológicas para la prevención del crimen. *Revista Escpogra PNP*. https://revistaescpograpnp.com/ojs/index.php/1/article/download/44/24

PERALTA, L. A. (2024): "Los usos criminales de los 'deepfakes' se disparan: estafas, pornografía y suplantación de identidad", *El País*, 2 de octubre. Disponible en: https://elpais.com/proyecto-tendencias/2024-10-02/los-usos-criminales-de-los-deepfakes-se-disparan-estafas-pornografia-y-suplantacion-de-identidad.html.

PROSEGUR RESEARCH (2024): *Innovación criminal*. Disponible en: https://www.prosegurresearch.com/blog/trends/innovacion-tecnologica-criminal.

ROJAS, J. (2016): "Innovación: Parábola y concepto", *Trilogía*. Disponible en: https://revistas.itm.edu.co/index.php/trilogia/article/download/181/187.

SÁNCHEZ, L. C. (2021): "Impacto de las innovaciones tecnológicas en la comunicación estratégica para la defensa y seguridad frente al terrorismo y las actividades ilícitas en las Américas", *Seguridad, Ciencia & Defensa*. Doi: ttps://doi.org/10.59794/rscd.2018.v4i4.44.

TAMAYO, D. (2023): *#CartelTikTok: How Drug Cartels Utilise Social Media*, University of Glasgow y Charles University. Disponible en: 120459758.pdf.

TAPIA SANDOVAL, A. (2025): "Niños sicarios: Estas son las razones por las que los cárteles mexicanos están llenando sus filas con ellos", *Infobae*, 11 de febrero. Disponible en: https://www.infobae.com/mexico/2025/02/11/estas-son-las-razones-por-las-que-los-carteles-mexicanos-estan-llenando-sus-filas-de-ninos-sicarios/.

UNITED NATIONS OFFICE ON DRUGS AND CRIME, UNODC (2024a): *Informe Mundial sobre las Drogas 2024*,

Disponible en: https://www.unodc.org/unodc/data-and-analysis/world-drug-report-2024.html.

— (2024b): *Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape,* Technical policy brief, octubre. Disponible en: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

VIÚDEZ, J. Y LORCA, J. (2024): *Cae una red criminal que desbloqueó y accedió a 1,3 millones de dispositivos, 30.000 de ellos en España*. *El País*, 19 de septiembre. Disponible en: https://elpais.com/espana/2024-09-19/cae-una-red-criminal-que-desbloqueo-y-accedio-a-13-millones-de-dispositivos-30000-de-ellos-en-espana.html.

WAINWRIGHT, T. (2018): *Narconomics: Cómo administrar un cártel de la droga*, Debate.

Fundación Carolina, septiembre 2025
Fundación Carolina
Plaza del Marqués de Salamanca nº 8
4ª planta, 28006 Madrid - España
www.fundacioncarolina.es
@Red_Carolina

https://doi.org/10.33960/AC_10.2025